



U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

CLAIM TO CONVENTION PRIORITY UNDER
35 U.S.C. § 119

Docket Number:
10191/2275

Conf. Number:
4797

Application Number
10/090,718

Filing Date
Mar. 4, 2002

Examiner
D. Cervetti

Art Unit
2136

Invention Title
**METHOD AND DEVICE FOR DATA ENCRYPTION
IN PROGRAMMING OF CONTROL UNITS**

Inventor(s)
Martin HURICH

Address to:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

A claim to the Convention Priority Date pursuant to 35 U.S.C. § 119 of Application No. 10 110049.3 filed in the German Patent Office on March 2, 2001 is hereby made. To complete the claim to the Convention Priority Date, a certified copy of the priority application is attached.

Dated: 8/21/06

By: Gerard A. Messina (Reg. No. 41,172)
Gerard A. Messina (Reg. No. 35,952)

KENYON & KENYON LLP
One Broadway
New York, N.Y. 10004
(212) 425-7200 (telephone)
(212) 425-5288 (facsimile)

CUSTOMER NO. 26646
PATENT TRADEMARK OFFICE

BUNDESREPUBLIK DEUTSCHLAND



BEST AVAILABLE COPY

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 101 10 049.3

Anmeldetag: 2. März 2001

Anmelder/Inhaber: ROBERT BOSCH GMBH, Stuttgart/DE

Bezeichnung: Verfahren und Vorrichtung zur Datenverschlüsselung
bei der Programmierung von Steuergeräten

IPC: H 04 L, G 05 B

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der
ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 19. Februar 2002
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Weihmayer

28.02.01

5

ROBERT BOSCH GMBH, 70442 Stuttgart

10

Verfahren und Vorrichtung zur Datenverschlüsselung bei der
Programmierung von Steuergeräten

Beschreibung

15

Die vorliegende Erfindung betrifft ein Verfahren und eine Vorrichtung zur Datenverschlüsselung bei der Programmierung von Steuergeräten.

20

Stand der Technik

25

Um zu verhindern, daß elektronisch gespeicherte Daten abgehört oder gar verändert werden, werden diese verschlüsselt. Ohne den entsprechenden Schlüssel zum Entschlüsseln können diese Daten dann nicht von einem Nichtberechtigten verwertet werden.

30

Bei der Programmierung von Steuergeräten wird ein Datenstrom über eine Datenleitung von einem Programmiergerät zu einem Steuergerät zu dessen Programmierung übertragen. Sowohl von Anwendern als auch vom Gesetzgeber werden mittlerweile Verfahren zur Verschlüsselung des Datenstroms gefordert. Auf diese Weise soll ein nicht bestimmungsgemäßer Zu-

griff auf den Inhalt der Speicherbausteine im Steuergerät verhindert werden.

5 Dabei ist zu beachten, dass das Verschlüsselungsverfahren geeignet sein soll, zusammen mit anderen Codierverfahren und Kompressionsverfahren verwendet zu werden, ohne an Wirksamkeit zu verlieren oder eine gegenseitige Behinderung der Verfahren zu verursachen.

10 Zu unterscheiden ist zwischen symmetrischen und asymmetrischen Verfahren. Bei den symmetrischen Verfahren wird ein Schlüssel sowohl zum Verschlüsseln als auch zum Entschlüsseln verwendet. Bei asymmetrischen Verfahren unterscheidet sich der Schlüssel zum Verschlüsseln von demjenigen zum
15 Entschlüsseln.

Bekannt ist ein symmetrisches, blockorientiertes Verschlüsselungsverfahren, bei dem wandernde XOR-Masken zur Verschlüsselung eingesetzt werden. Dieses Verfahren zeichnet
20 sich durch seine Einfachheit aus und eignet sich daher besonders für den Einsatz in Steuergeräten. Nachteilig ist dabei, dass größere Bereiche bekannter Daten (z. B. Füllbereiche, welche meistens aus FFh oder 00h bestehen) dem potentiellen Angreifer den Schlüssel verraten können. Beson-
25 ders bei der Verwendung von Kompressionsverfahren, welche auf dem Huffman-Coding basieren, treten üblicherweise längere Ketten gleicher Bits auf. Dies erleichtert dem Angreifer die Entschlüsselung des Codes.

30 Aus der US-Patentschrift 5,724,428 ist ein Verfahren zur Übertragung von Daten bekannt, welches eine Verschlüsselung und Entschlüsselung der übertragenen Daten ermöglicht. Die Druckschrift beschreibt die Verwendung eines geheimen Schlüssels, welcher wiederum in verschlüsselter Form vom

Sender zum Empfänger übertragen wird. Dieser geheime Schlüssel wird im weiteren dazu verwendet, um die zu übertragenden Daten zu verschlüsseln und zu entschlüsseln.

5 Das Verschlüsselungsverfahren an sich verwendet ein Feld von beliebiger Größe, welches mit den zu verschlüsselnden Werten verknüpft wird. Hierbei ist von Bedeutung, dass die zu verschlüsselnden Daten zunächst in erste und zweite Worte aufgeteilt werden. Diese Worte haben beliebige, aber feste
10 Längen. Anschließend wird auf diese Worte eine invertierbare Operation angewandt. Dabei werden zunächst die ersten Worte mit dem ersten Element des oben beschriebenen Feldes verknüpft und dann die zweiten Worte mit dem zweiten Element des Feldes verknüpft. Anschließend werden die Worte
15 wechselweise über die invertierbare Operation miteinander verknüpft und danach um jeweils die Anzahl von Stellen rotiert, welche dem jeweils anderen Wort entspricht. Danach wird das jeweils nächste Element des oben beschriebenen Feldes zu den Worten addiert.

20 Da die zu verschlüsselnden Daten in erste und zweite Worte aufgeteilt werden, kann dieses Verfahren nicht auf einzelne Bytes angewendet werden. Die Tatsache, dass jedesmal der Schlüssel mit übertragen werden muss, erweist sich als auf-
25 wendig und riskant.

Die vorliegende Erfindung soll ein alternatives Verfahren und eine Vorrichtung zur Datenverschlüsselung bei der Programmierung von Steuergeräten angeben.

30

Vorteil der Erfindung

Das erfindungsgemäße Verfahren nach Anspruch 1 zeichnet sich dadurch aus, dass die zu übertragenden Daten zunächst

in einem Programmiergerät mit einem ersten Schlüssel verschlüsselt werden, die verschlüsselten Daten über eine Datenleitung zu einem Steuergerät übertragen werden und die Daten in dem Steuergerät mit einem zweiten Schlüssel, der
5 im Steuergerät vorgesehen ist, entschlüsselt werden.

Dadurch, dass der Schlüssel nicht mitübertragen wird, sondern bereits im Steuergerät vorgesehen ist, verringert sich die zu übertragende Datenmenge und erhöht sich die Sicherheit.
10

Eine erfindungsgemäße Vorrichtung zur Datenverschlüsselung bei der Programmierung von Steuergeräten weist ein Programmiergerät auf, bei dem ein erster Schlüssel vorgesehen ist,
15 ein Steuergerät, bei dem ein zweiter Schlüssel vorgesehen ist und eine Datenleitung zur Übertragung der verschlüsselten Daten.

Vorteilhafte Ausgestaltungen der Erfindung ergeben sich aus den Unteransprüchen sowie aus der Beschreibung.
20

Bei dem erfindungsgemäßen Verfahren kann sowohl ein symmetrisches Verschlüsselungsverfahren als auch ein asymmetrisches Verschlüsselungsverfahren zur Anwendung kommen. Sind
25 der erste und der zweite Schlüssel identisch, so handelt es sich um ein symmetrisches Verschlüsselungsverfahren. Sind der erste und zweite Schlüssel nicht identisch, findet ein asymmetrisches Verschlüsselungsverfahren Anwendung.

Bevorzugt wird für die Verschlüsselung eine Tabelle S mit m Elementen S_0 bis S_{m-1} verwendet. Auf diese Tabelle wird mittels einer Hash-Funktion $h(x)$ zugegriffen. $h(x)$ dient dabei als Index.
30

Ein verschlüsseltes Byte n^* wird aus einem unverschlüsselten Byte n nach folgender Vorschrift gebildet (Für Entschlüsselung und Verschlüsselung ist ein Startwert n_{-1} notwendig):

5

$$n_{-1} \equiv S_0 \quad (\text{Formel 1})$$

$$n_i^* = \left(n_i \lll \sum_{j=0}^i n_{j-1}^* \right) \oplus S_{h\left(\sum_{j=0}^i n_{j-1}^*\right)} \quad (\text{Formel 2})$$

- 10 Aus einem verschlüsselten Byte n^* wird das unverschlüsselte Byte n nach folgender Vorschrift gebildet:

$$n_i = \left(n_i^* \oplus S_{h\left(\sum_{j=0}^i n_{j-1}^*\right)} \right) \ggg \sum_{j=0}^i n_{j-1} \quad (\text{Formel 3})$$

- 15 Der Schlüssel kann sowohl als elektronischer Schaltkreis, beispielsweise in einem ASIC, implementiert sein als auch als Computerprogramm vorliegen.

- 20 Das Computerprogramm kann auf geeigneten Datenträgern, wie EEPROMs, Flash-Memories aber auch CD-ROMs, Disketten oder Festplattenlaufwerken gespeichert sein. Abgearbeitet wird das Computerprogramm von einer elektronischen Recheneinheit, zum Beispiel einem Mikroprozessor, im Programmiergerät bzw. Steuergerät.

25

Bevorzugt weisen das Programmiergerät und das Steuergerät jeweils eine elektronische Recheneinheit und einen Speicherbaustein auf, die über einen Datenbus miteinander ver-

bunden sind. Als elektronische Recheneinheit dient beispielsweise ein Mikroprozessor.

5 Auch für den Fall, dass der Schlüssel vom Sender zum Empfänger übertragen wird, eignet sich als Schlüssel eine Tabelle, auf die mittels einer Hash-Funktion zugegriffen wird.

10 Zeichnungen

Die Erfindung wird anhand der beigefügten Zeichnung näher erläutert. In dieser zeigt:

15 Figur 1 eine bevorzugte Ausführungsform der erfindungsgemäßen Vorrichtung in schematischer Darstellung, und

20 Figur 2 eine bevorzugte Ausführungsform des erfindungsgemäßen Verfahrens im Flussdiagramm.

Figur 1 zeigt schematisch den Aufbau einer erfindungsgemäßen Vorrichtung. Zu erkennen sind ein Programmiergerät 10, ein Steuergerät 11 und eine Datenleitung 12. Weiterhin sind
25 im Programmiergerät 10 ein Mikroprozessor 13 und ein Speicherelement 14 zu erkennen, die über einen Datenbus 15 miteinander verbunden sind. Ein vergleichbarer schematischer Aufbau findet sich ebenfalls im Steuergerät 11. In diesem sind ein Mikroprozessor 16, ein Speicherbaustein 17 und ein
30 Datenbus 18 dargestellt.

Nachfolgend wird die Funktionsweise der erfindungsgemäßen Vorrichtung erläutert:

Im Speicherbaustein 14 des Programmiergeräts 10 sind Daten zur Programmierung des Steuergeräts 11 abgelegt. Mittels einer Tabelle und einer Hash-Funktion, die ebenfalls im Speicherbaustein 14 gespeichert sind, werden die Daten mit dem Mikroprozessor 13 verschlüsselt.

Das Verfahren bedient sich dabei folgender reversibler Operationen:

- 10 - linksseitige Rotation (innerhalb eines Bytes): <<<
- rechtsseitige Rotation (innerhalb eines Bytes): >>>
- byteweises exklusives Oder: \oplus

15

Die Ergebnisse seien dabei invariant bezüglich Rotation um Vielfache von 8.

Für die Verschlüsselung wird eine Tabelle S mit m Elementen S_0 bis S_{m-1} verwendet. Auf diese Tabelle wird mittels einer Hash-Funktion $h(x)$ zugegriffen. $h(x)$ dient dabei als Index.

Zur einfacheren Beschreibung werden die während der Verschlüsselung aufeinanderfolgenden Bytes mit einem Index i , mit $i = 0, 1, 2, \dots$ versehen.

Ein verschlüsseltes Byte n^* wird aus einem unverschlüsselten Byte n nach folgender Vorschrift gebildet (Für Entschlüsselung und Verschlüsselung ist ein Startwert n_{-1} notwendig):

$$n_{-1} \equiv S_0$$

(Formel 1)

$$n_i^* = \left(n_i \lll \sum_{j=0}^i n_{j-1}^* \right) \oplus S_{h\left(\sum_{j=0}^i n_{j-1}^*\right)} \quad (\text{Formel 2})$$

Die verschlüsselten Daten werden anschließend über die Datenleitung 12 zum Steuergerät 11 übertragen. Werden die Daten bei der Übertragung abgehört, ist dies unschädlich, da die verschlüsselten Daten ohne den Schlüssel, der nicht mit übertragen wird, nicht verwertet werden können.

Die verschlüsselten Daten werden im Speicherbaustein 17 des Steuergeräts 11 gespeichert. Im Speicherbaustein 17 befindet sich der gleiche Schlüssel wie im Speicherbaustein 14 des Programmiergerät 10. Mit diesen werden die Daten wieder entschlüsselt.

Aus einem verschlüsselten Byte n^* wird das unverschlüsselte Byte n nach folgender Vorschrift gebildet:

$$n_i = \left(n_i^* \oplus S_{h\left(\sum_{j=0}^i n_{j-1}^*\right)} \right) \ggg \sum_{j=0}^i n_{j-1}^* \quad (\text{Formel 3})$$

Anschließend kann das Steuergerät 11 programmiert werden. Dabei werden die entschlüsselten Daten mit dem Mikroprozessor 16 abgearbeitet.

Das Flussdiagramm in Figur 2 verdeutlicht den Ablauf des erfindungsgemäßen Verfahrens.

In einem Schritt 20 wird zunächst die Verschlüsselung der Daten, welche zur Programmierung des Steuergeräts vorgesehen sind, durchgeführt. Die zu verschlüsselnden Daten wer-

den dabei nicht, wie dies wie im Stand der Technik beschrieben ist, in erste und zweite Worte aufgeteilt. Dadurch kann das Verfahren auch auf einzelne Bytes angewendet werden. Das Verfahren wendet eine Rotation um eine Anzahl
5 von Stellen an, welche von der gesamten Vorgeschichte der Verschlüsselung abhängig ist. Die Verschlüsselung eines Bytes ist somit nicht vorbestimmt sondern abhängig von der Vorgeschichte.

10 Die Elemente des Feldes werden nicht in linearer Reihenfolge eingesetzt, sondern über eine Hash-Funktion ausgewählt. Die Verknüpfung erfolgt nicht additiv, sondern über ein exklusives Oder. Ein zusätzlicher Parameter ist nicht die Anzahl der Operation, sondern die Auswahl der Hash-Funktion.
15 Dies reduziert die Laufzeit erheblich.

In einem anschließenden Verfahrensschritt 21 erfolgt die Datenübertragung über die Datenleitung 12. Da die übertragenen Daten verschlüsselt sind, sind sie für einen möglichen Angreifer nicht zu verwerten.
20

Anschließend werden in einem Verfahrensschritt 22 die Daten eingelesen, d.h. im Speicherbaustein 17 des Steuergeräts 11 abgelegt.
25

Abschließend erfolgt in einem Schritt 23 die Entschlüsselung der Daten. Der Schlüssel zum Entschlüsseln ist als Computerprogramm im Speicherbaustein des Steuergeräts 11 abgelegt.
30

Zur Entschlüsselung wird der gleiche Schlüssel wie derjenige zum Verschlüsseln verwendet. Es handelt sich somit hier um ein symmetrisches Verfahren.

Im Vergleich zum oben beschriebenen Verfahren, bei welchem wandernde XOR-Masken zur Verschlüsselung eingesetzt werden, wird der Schlüssel nicht in dem Datenstrom oder zusammen mit sonstigen Parametern übertragen, sondern befindet sich
5 bereits im Steuergerät. Außerdem wird keine Tabelle anhand solcher Parameter aus Pseudozufallszahlen generiert.

Im Gegensatz zu bekannten Verfahren erfolgt keine Addition von Schlüsselwerten während der Ver- und Entschlüsselung.
10 Beim erfindungsgemäßen Verfahren werden die Eingangswerte nicht auf zwei oder mehr Register zerteilt, um diese danach simultan zu verändern.

Das erfindungsgemäße Verfahren zeichnet sich dadurch aus,
15 dass der Schlüssel, in diesem Fall die Tabelle und die Hash-Funktion, nicht im Datenstrom über die Datenleitung übertragen wird, sondern sich bereits im Steuergerät befindet.

20 Da das beschriebene Verfahren die Eingangswerte nicht auf zwei oder mehr Register verteilt, um diese danach simultan zu verändern, kann es auch auf einzelne Bytes angewendet werden, dies ist insbesondere im Rahmen der Anwendung innerhalb der Flashprogrammierung vorteilhaft.

25 Typischerweise wird das erfindungsgemäße Verfahren von einer Vielzahl von Anwendern eingesetzt werden. Deshalb muss sichergestellt sein, dass ein versehentlicher Datenaustausch zwischen verschiedenen Anwendern vermieden wird.
30 Aufgrund der Tatsache, dass das beschriebene Verfahren parametrisierbar ist, kann dies vermieden werden.

Mit dem Verfahren sind große Bereiche mit gleichem Inhalt (Füllbereiche) sicher zu verschlüsseln. Die kodierte Be-

reiche geben keinen Aufschluß über den verwendeten Schlüssel. Eine byteweise Zuordnung zwischen Ein- und Ausgangsdaten ist nicht möglich.

- 5 Das Verfahren erfordert keinen temporären Speicherplatz für den Datenstrom bzw. Teile daraus. Lediglich ein Byte wird als Speicherplatz für die laufende Summe benötigt. Auch der Bedarf an Code für die Entschlüsselung ist sehr gering (ca. 130 Bytes). Für den Einsatz in Kfz-Steuergeräten ist dies
- 10 von großer Bedeutung.

- Es ist auch möglich, durch Verwendung einer benutzerspezifischen Tabelle das Verfahren an unterschiedliche Anforderungen anzupassen. Zusätzlich kann eine beliebige Hash-
- 15 Funktion für den Tabellenzugriff verwendet werden, um mögliche Rückschlüsse auf den Inhalt der Tabelle zu erschweren.

- Der Datendurchsatz bei dem beschriebenen System liegt bei-
- 20 spielsweise bei mehr als 7 MB/Minute.

28.02.01

ROBERT BOSCH GMBH, 70442 Stuttgart

5

Ansprüche

1. Verfahren zur Datenverschlüsselung bei der Programmierung von Steuergeräten (11), bei dem die zu übertragenden
10 Daten in einem Programmiergerät (10) mit einem ersten Schlüssel verschlüsselt werden, die verschlüsselten Daten über eine Datenleitung (12) zu einem Steuergerät (11) übertragen werden und die Daten in dem Steuergerät (11) mit einem zweiten Schlüssel, der im Steuergerät (11) vorgesehen
15 ist, entschlüsselt werden.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der erste und der zweite Schlüssel identisch sind.
- 20 3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der erste und der zweite Schlüssel nicht identisch sind.
4. Verfahren nach Anspruch 2, dadurch gekennzeichnet,
25 dass als Schlüssel eine Tabelle verwendet wird, auf die mittels einer Hash-Funktion zugegriffen wird.
5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass mindestens einer der Schlüssel in einer elektronischen Schaltung implementiert ist.
30
6. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass mindestens einer der Schlüssel als Computerprogramm vorliegt.

7. Vorrichtung zur Datenverschlüsselung bei der Programmierung von Steuergeräten, mit einem Programmiergerät (10), bei dem ein erster Schlüssel vorgesehen ist, einem Steuergerät (11), bei dem ein zweiter Schlüssel vorgesehen ist und einer Datenleitung (12) zur Übertragung der verschlüsselten Daten.

8. Vorrichtung nach Anspruch 7, dadurch gekennzeichnet, dass der erste und der zweite Schlüssel identisch sind.

9. Vorrichtung nach Anspruch 7, dadurch gekennzeichnet, dass der erste und der zweite Schlüssel nicht identisch sind.

10. Vorrichtung nach einem der Ansprüche 7 bis 9, dadurch gekennzeichnet, dass das Programmiergerät und das Steuergerät jeweils eine elektronische Recheneinheit (13, 16) und einen Speicherbaustein (14, 17) umfassen, die über einen Datenbus (15, 18) miteinander verbunden sind.

11. Computerprogramm mit Programmcode-Mitteln, um die Verschlüsselung mittels einer Tabelle und einer Hash-Funktion durchzuführen, wenn das Computerprogramm auf einer entsprechenden Recheneinheit, insbesondere in einer elektronischen Recheneinheit in einem Programmiergerät (10) ausgeführt wird.

12. Computerprogramm mit Programmcode-Mitteln, um die Entschlüsselung mittels einer Tabelle und einer Hash-Funktion durchzuführen, wenn das Computerprogramm auf einer entsprechenden Recheneinheit, insbesondere in einer elektronischen Recheneinheit in einem Steuergerät (11) ausgeführt wird.

13. Computerprogrammprodukt mit Programmcode-Mitteln, die
auf einem computerlesbaren Datenträger gespeichert sind, um
die Verschlüsselung mittels einer Tabelle und einer Hash-
Funktion durchzuführen, wenn das Computerprogramm auf einer
5 elektronischen Recheneinheit, insbesondere einer elektroni-
schen Recheneinheit eines Programmiergerätes (10) ausge-
führt wird.

10 14. Computerprogrammprodukt mit Programmcode-Mitteln, die
auf einem computerlesbaren Datenträger gespeichert sind, um
die Entschlüsselung mittels einer Tabelle und einer Hash-
Funktion durchzuführen, wenn das Computerprogramm auf einer
elektronischen Recheneinheit, insbesondere einer elektroni-
schen Recheneinheit eines Steuergerätes (11) ausgeführt
15 wird.

20

25

30

5 28.02.01

ROBERT BOSCH GMBH, 70442 Stuttgart

10 Verfahren und Vorrichtung zur Datenverschlüsselung bei der
Programmierung von Steuergeräten

Zusammenfassung

15

Es werden ein Verfahren und eine Vorrichtung zur Datenverschlüsselung bei der Programmierung von Steuergeräten beschrieben.

20 Bei dem Verfahren werden die zu übertragenden Daten byte-
weise in einem Programmiergerät mit einem ersten Schlüssel
verschlüsselt und anschließend über eine Datenleitung zu
einem Steuergerät übertragen. Abschließend werden die Daten
in dem Steuergerät (11) mit einem zweiten Schlüssel, der im
25 Steuergerät (11) vorgesehen ist, entschlüsselt.

(Figur 1)

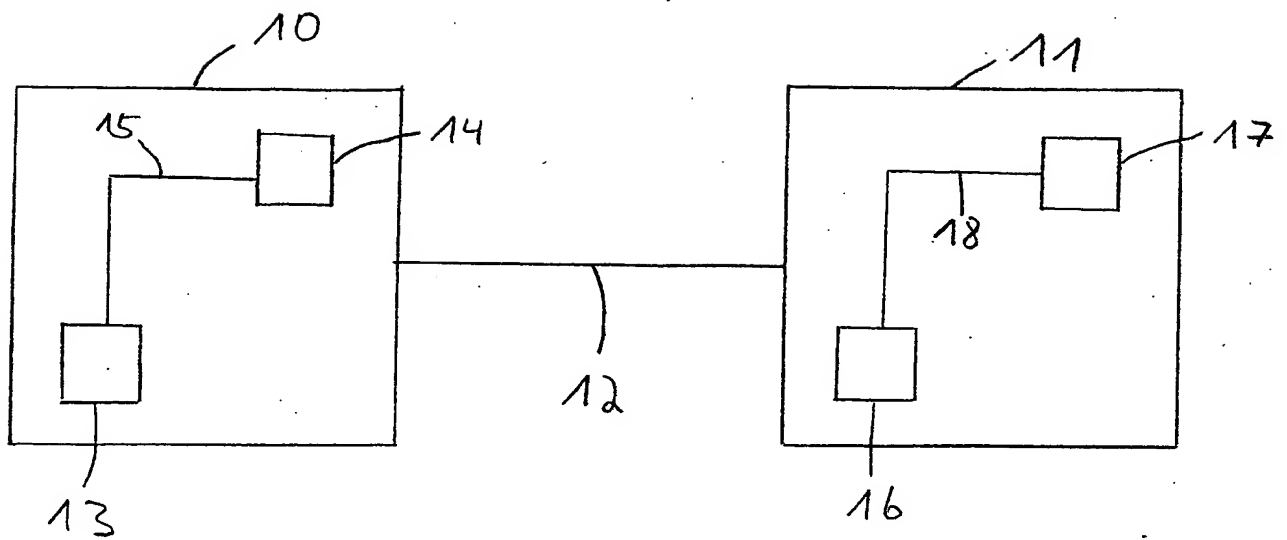


Fig. 1

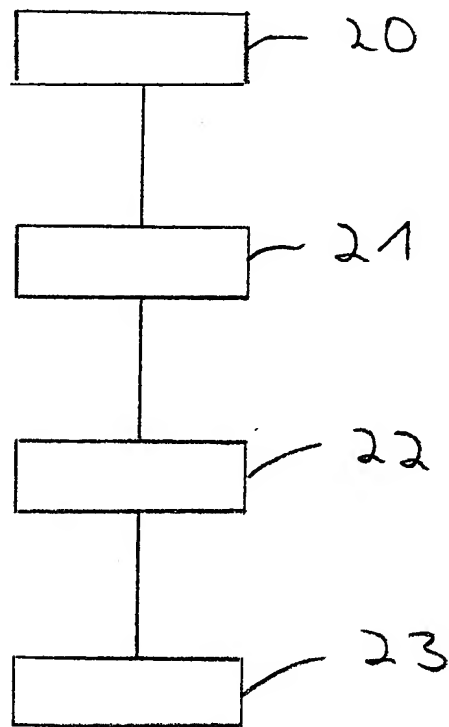


Fig. 2